Virus and Malicious Logic Incident Response Procedures

April 2001

Purpose

The purpose of this procedure is to outline the process to be followed when a virus or other form of malicious logic (hereafter referred to in the generic "virus") is identified in the State of Iowa enterprise or ITD systems. This procedure may be changed or otherwise updated at any time.

Preliminary Activities

1. A standard e-mail account for virus reporting will be used. This account will be utilized to both send and receive reports of viral activity. In addition, ITD will use it to identify recommended countermeasures. This account has been established as ITDAlert@itd.state.ia.us.

2. A standard mailing list will be developed by ITD to get information to the agencies in a timely manner. An effort will be made to ensure each agency is represented on this mailing list. The list will also include phone numbers to facilitate communication in the event that e-mail capabilities are unavailable. Updates should be made by the agencies through ITD ALERT.

3. Each participating agency will be notified and given a copy of this procedure. It will also be maintained on the enterprise security web site, along with a link to facilitate mailing of alerts.

Procedure

1. Upon virus notification, as many team members as are available will gather to discuss the situation. The following issues will be addressed prior to notification of the event:

   a. Is it a real virus or a hoax?
   b. What systems are vulnerable?
   c. What is the severity of the virus?
   d. What does the virus do?
   e. What are distinguishing characteristics of the virus?
   f. Is it quarantined by current virus signatures?
   g. If not, are there alternate fixes?
   h. What are the recommended courses of action?

2. State agencies and customers will be notified via the ITD ALERT e-mail ID. The alert will contain information gathered during Step 1 such that personnel receiving the report may make an educated decision on next steps. The e-mail will also identify a point of contact for that particular event.

3. Once the alert is sent out, or concurrent with the notification, any necessary corrective actions will be performed on ITD and customer systems. Significant changes in status or other developments should be shared with the enterprise as necessary.

4. A final e-mail will be sent out once the event reaches a conclusion. Any lessons learned or other identifying characteristics should be indicated.